

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

-----X

UNITED STATES OF AMERICA :

V. :

13Cr. 616 (VLB)

JOHANNES THALER, :

Defendant. :

-----X

**DEFENDANT JOHANNES THALER'S REPLY TO GOVERNMENT'S  
MEMORANDUM IN OPPOSITION TO DEFENSE MOTIONS TO SUPPRESS**

**JASON SER, ESQ.**

Federal Defenders of New York  
Attorney for Defendant

**JOHANNES THALER**

300 Quarropas Street, Room 260  
White Plains, New York 10601  
Tel.:(914) 428-7126

**JASON SER, ESQ.**

Of Counsel

TO: **PREET BHARARA, ESQ.**  
United States Attorney for the  
Southern District of New York  
One St. Andrew's Plaza  
New York, New York 10007

Attn: **BENJAMIN ALLEE, ESQ.**  
Assistant United States Attorney

## TABLE OF CONTENTS

	<u>Page</u>
I. The Government’s Probable Cause Argument Fails . . . . .	Page -1-
A. The Four Corners of the June Yahoo Warrant Do Not Include Facts Being Asserted by the Government in Support of Probable Cause . . . . .	Page -1-
B. Because the “Totality of the Circumstances” Standard Applies to Magistrate Approval of a Search Warrant, Probable Cause Cannot Be a One-way Ratchet . . . . .	Page -2-
II. The Court Should Suppress All the Seized Electronic Materials or Conduct a Hearing to Determine the Actual Scope and Conduct of Electronic Searches . . . . .	Page -4-
III. The Good Faith Exception Does Not Apply in this Case . . . . .	Page -9-
A. The June Yahoo Warrant Lacked Any Indicia of Probable Cause . . . . .	Page -10-
B. Even If Probable Cause Exists, the Warrant Was “So Facially Deficient – I.e., in Failing to Particularize the Place to Be Searched or the Things to Be Seized – That the Executing Officers Cannot Possibly Presume it to Be Valid.” . . . . .	Page -11-
1. The June Yahoo Warrant Incorporates Only “Section Ii of Attachment B,” Which Authorizes the Wholesale Search of Mr. Thaler’s Yahoo Email Account Untethered from Any Violation of Law . . . . .	Page -11-
2. The Exclusionary Rule Applies Due to the Lack of Particularity . . . . .	Page -15-
IV. An Evidentiary Hearing Is Warranted to Resolve Several Factual Disputes . . . .	Page -18-
V. Conclusion . . . . .	Page -19-

Mr. Thaler files the instant reply brief to address points raised by the government in its responsive entitled “Omnibus Memorandum of Law of the United States of America in Opposition to Defendants’ Pretrial Motions.” (hereinafter “Gov’t Brief”). Mr. Thaler filed his Motions to Suppress Evidence (hereinafter “Mot. to Supp.”) together with exhibits on May 12, 2014.

**I.**

**THE GOVERNMENT’S PROBABLE CAUSE ARGUMENT FAILS**

The government’s arguments with regard to the existence of probable cause fail in two respects. First, the government exceeds the four corners of the June Yahoo Warrant application in an effort to justify the magistrate court’s finding of probable cause. Second, the government fails to explain why the Court should not consider, under the “totality of the circumstances,” that searches of Lustyik’s email account (and even Taylor’s), which occurred prior to June Yahoo Warrant, did not reveal any more specific emails from or to Mr. Thaler discussing Mr. Lustyik’s obstruction of the Utah investigation.

**A. The Four Corners of the June Yahoo Warrant Do Not Include Facts Being Asserted by the Government in Support of Probable Cause.**

The government makes various factual assertions in its brief to support the magistrate’s probable cause finding with regard to the June Yahoo Warrant for Mr. Thaler’s email account. For example, the government claims that

[t]he investigation further revealed that at the time Lustyik made these attempts to interfere with the investigation of Taylor, Lustyik, Thaler, and Taylor were in a business relationship, and that Lustyik *expected* that his assistance in heading off the investigation of Taylor would result in personal profit in Lustyik’s business dealings with Taylor.

Gov’t Brief at 8 (emphasis added). Problematically, no such factual assertion appears in the four

corners of the affidavit.<sup>1</sup> See Illinois v. Gates, 462 U.S. 213, 238 (1983) (probable cause assessments are to be made from “all the circumstances set forth in the affidavit”); United States v. Gourde, 440 F.3d 1065, 1067 (9th Cir.2006) (en banc) (“All data necessary to show probable cause for the issuance of a search warrant must be contained within the four corners of a written affidavit given under oath”); see also United States v. Falso, 544 F.3d 110, 122 (2d Cir. 2008) (citing Gourde for parenthetical’s proposition). Agent Hopkins does not couch any probable cause claim in the context of a quid pro quo-style relationship between Lustyik and Taylor as motivating the former to obstruct a federal investigation of the latter.

Immediately thereafter in its brief, the government claims that

[i]n addition, the investigation revealed that *Thaler*, Lustyik’s long-time friend, assisted in the corrupt, fraudulent arrangement between Lustyik and Taylor, *relaying messages between them about Lustyik’s efforts to derail the Utah case, and Taylor’s intentions to pay Lustyik.*

Gov’t Brief at 8. It is unclear where within Agent Hopkins’ affidavit such a claim exists. He did not state that Mr. Thaler relayed messages between Lustyik and Taylor about any efforts to derail the Utah case.

**B. Because the “Totality of the Circumstances” Standard Applies to Magistrate Approval of a Search Warrant, Probable Cause Cannot Be a One-Way Ratchet.**

The government correctly points out that a judge prior to issuing a search warrant “should take into account the ‘totality-of-the-circumstances’ and his consideration should include an ‘assessment of probabilities in *particular factual contexts*.’” Gov’t Brief at 26 (quoting Gates, 462 U.S. at 232-33) (emphasis added). The “totality-of-the-circumstances” cannot mean, as the

---

<sup>1</sup> Should the government somehow rely upon such assertions as a basis for any good faith exception, which Mr. Thaler does not concede applies, then an evidentiary hearing is necessary to provide testimony from an appropriate witness to this effect.

Government seems to believe, that the magistrate court looks only to probable cause inferences arising from the facts. Instead, a magistrate must weigh the suspicious with the countervailing innocent inferences of the evidence. Simply put, probable cause is not a one-way ratchet. Thus, the Government ignores how some of the established facts conflict with and lessen the purported probable cause implications of other facts.

By the time of Agent Hopkins' affidavit for the June Yahoo Warrant, the government already had executed search warrants for email accounts belonging to Lustyik and Taylor. By virtue of Agent Hopkins' affidavit and its contents, it is apparent that those email accounts had been thoroughly examined. Certainly the fact that no more specific emails (or even less specific for that matter) involving Mr. Thaler discussed obstructive conduct by Lustyik with regard to the Utah case has significance. This omission is curious at the least. As a result, when the single email cited by Agent Hopkins is read in this particular factual context, i.e., no other more specific emails, it does not go as far as the government needs it to for demonstrating probable cause. And, despite the government claiming that emails about the business relationship between and among Mr. Thaler, Lustyik and Taylor "was more than sufficient to demonstrate a fair probability that evidence of *a crime* would be found in Thaler's Email Account," Gov't Brief at 29 (emphasis added), that is not the legal standard. It must have been evidence of the crime identified in the search warrant application. See United States v. Travisano, 724 F.2d 341, 345 (2d Cir.1983) ("To establish probable cause to search a residence, two factual showings are necessary-first, that a crime was committed and second, that there is probable cause to believe that evidence of such a crime is located at the residence.").

## II.

### **THE COURT SHOULD SUPPRESS ALL THE SEIZED ELECTRONIC MATERIALS OR CONDUCT A HEARING TO DETERMINE THE ACTUAL SCOPE AND CONDUCT OF ELECTRONIC SEARCHES**

The government argues that searches of Mr. Thaler's Yahoo email account and his iPhone did not constitute a "general rummaging" and rather was consistent with "procedure intended by the law." Gov't Brief at 41. In summarizing what the government did with regard to its searches of the email account and iPhone, the government explains that "the Government obtained all of the contents of Lusyk's and Thaler's email accounts, searched them for responsive items, and then produced the entirety of the accounts in discovery . . . ." *Id.* This list is incomplete, however. The *complete* manner in which the searches occurred constituted a "general rummaging." See United States v. Ganius, – F.3d –, 2014 WL 2722618 (2d Cir. June 17, 2014).

During the evidentiary hearing in Utah, Agent Hopkins testified that the search returns for the June Yahoo Warrant produced emails from Mr. Thaler's Yahoo account that were "not responsive" to items listed for seizure in Attachment B. See Mot. to Supp. Exhibit I at 407. Rather than returning the emails that were "not responsive" to Yahoo or Mr. Thaler, however, Agent Hopkins testified that "all of the e-mails [were eventually] loaded up into Relativity" and made subject to repeated searches by law enforcement around the country as various investigations continued. *Id.* at 343, 360-64. Agent Hopkins testified that a forensic report detailing the contents of Mr. Thaler's iPhone also contained "both relevant and irrelevant data" relative to what the search warrant specified for seizure from within the iPhone. *Id.* at 360. His testimony suggests that all of the iPhone data was uploaded into Relativity. Finally, Agent Hopkins expressly testified that "not responsive" returns were stored for continual review and at times were reclassified as responsive as

new information derived from several ongoing investigations put that evidence into context. Id. at 360-64.

Despite this express testimony, the government claims that “the searches were proper” and invokes 18 U.S.C. § 2703 to somehow justify the scope of and conduct related to the search warrant’s execution. Gov’t Brief at 39-40. Curiously, it omits the fact that Mr. Thaler’s Yahoo email account and contents of his iPhone were uploaded and stored in Relativity and repeatedly searched when describing the chain of events vis a vis the search warrants at issue. Gov’t Brief at 41. And wrongly, it claims that the defense “point[s] to no evidence that resulted from the alleged ‘general rummaging.’” Gov’t Brief at 42. The government makes no argument with regard to Agent Hopkins’ testimony above and fails to explain how such searches were lawful despite the Utah district court ordering: (1) suppression of evidence Utah prosecutors volunteered to withhold; (2) removal of certain evidence from Relativity; and (3) ceasing further Relativity searches. See Gov’t Brief, Exhibit J at 31. It has not explained how any repeated searches in the absence of a new search warrant application are lawful and reasonable under the Fourth Amendment. It has not explained how keeping evidence that is “not responsive” is lawful and reasonable under the Fourth Amendment. Defendants are entitled to information about the conduct of the search to ensure that overbroad, general searches -- in which the government can examine any document at its whim -- are not occurring.

Though the government argues that § 2703 permits it to compel production of “*all* emails, opened and unopened, without date restriction, in an email account,” id. at 40 (emphasis added), nothing in the statute identifies an “all” or nothing proposition with regard to what may or has to be sought by search warrant. The government also cites no case law for this “all” or nothing

proposition. It appears to be an attempt to sidestep the larger issue regarding the manner in which the search of Mr. Thaler's Yahoo email account was executed and what was done with the "not responsive" evidence.<sup>2</sup> Nothing in § 2703 precluded the government from requesting a more limited series of emails consistent with a more particular list of characteristics relevant to the suspected crime, e.g., the email addresses or names of individuals sending email to Mr. Thaler or receiving email from Mr. Thaler. This could have prevented the general rummaging that ensued. It also would have made it impossible for the government to then keep and upload for continual review "not responsive" evidence. Unlike Utah prosecutors in the Utah case, the government here has not agreed to forego use of certain articles of evidence obtained as a result of the search warrants.

Simply because the materials involved here are largely in electronic form does not relieve the Government of its constitutional responsibility to conduct appropriately narrow searches and to determine the limited subset of items to be seized within a reasonable time. Just this week, the Second Circuit issued a very important new Fourth Amendment case, United States v. Ganius, – F.3d –, 2014 WL 2722618 (2d Cir. June 17, 2014). The Court considered "whether the Fourth Amendment permits officials executing a warrant for the seizure of particular data on a computer to seize and indefinitely retain every file on that computer for use in future criminal investigations. [The Court] h[e]ld that it does not." Id. at \*10.

In an opinion by Judge Chin, the Court held that the government violates the Fourth Amendment when it indefinitely retains computer files that were seized pursuant to a search warrant

---

<sup>2</sup> It is especially concerning given that Agent Hopkins' investigation focused on obstruction-related conduct rather than the conduct giving rise to the charges in the instant case. It is problematic if any evidence relevant to the instant case was recovered from Mr. Thaler's Yahoo email account or his iPhone, but was "not responsive" to the obstruction-based search warrant. An evidentiary hearing is required to make a determination in this regard.

but are not responsive to the warrant. Id. at \*12. Admittedly, courts have long held that the practicality of computer search and seizure allows government agents to seize computers and search them later for responsive files. In Ganias, however, the Second Circuit makes clear that the government's right to overseize is temporary, and that it has no right to continue to retain the non-responsive files indefinitely. Id. "Perhaps the 'wholesale removal' of intermingled computer records is permissible where off-site sorting is necessary and reasonable, . . . but this accommodation does not somehow authorize the Government to retain all non-responsive documents indefinitely, for possible use in future criminal investigations." Id. (citation omitted). The court does not say exactly when the government has to destroy, delete, or return its copy of the non-responsive files. But the Court does make clear that the government has such a duty: Continued retention of the files is a Fourth Amendment "seizure," the Court held, and eventually the retention goes on for so long that the retention is unreasonable. Id. at \*10-12. Put simply, individuals have a right to the deletion or return of non-responsive computer files as a matter of Fourth Amendment reasonableness.

The Court also determined that the exclusionary rule applied. First, the government effected a widespread seizure of files beyond the warrant's scope that resembled "an impermissible general search." Id. at \*12. Second, the agents did not act in good faith given their awareness that non-responsive items had to be purged, but intentionally retained them nonetheless. Id. Third, the benefits of deterrence "are great." Id. at \*13. The Court explained that "[w]ith the Government's use of forensic mirror images becoming increasingly common, deterring its unconstitutional handling of non-responsive data has grown in importance." Id. Fourth, the costs of suppression were "minimal" because "[t]his is not a case where a dangerous defendant is being set free." Id.

Even before this decision, district courts within the Second Circuit have emphasized that they will scrutinize the treatment of “overseized” data to ensure that the government has performed searches designed to ensure compliance with a particularized warrant. See United States v. Graziano, 558 F.Supp.2d 304, 315 (E.D.N.Y. 2008). For example, the Graziano court emphasized:

[T]here are Fourth Amendment limits to every search that apply with equal force to searches of computers. Thus, although courts are ill-suited to manage in advance how the computer will be searched, law enforcement must establish the basis for searching the computer and particularize the evidence being sought.

Graziano, 558 F.Supp.2d at 316; see also United States v. Debbi, 244 F.Supp.2d 235, 237 (S.D.N.Y. 2003) (holding by Judge Rakoff that suppression of all seized materials that the Government had not shown to be within the scope of the warrant, and scheduled a hearing to determine whether *all* seized items should be suppressed).

The Government’s conduct in this case far exceeds any standard of reasonableness. Not only did the searches of Mr. Thaler’s Yahoo email account and iPhone exceed what was responsive to the search warrants by Agent Hopkins’ own admissions, but the non-responsive material from the Yahoo email account and iPhone were kept continuously by the government in an online database that was subject to unlimited and repeated searches by multiple offices and agencies investigating *different* crimes.<sup>3</sup> This included federal prosecutors. Exhibit I at 408. By Agent Hopkins’ own admission,

---

<sup>3</sup> At the Utah evidentiary hearing, Agent Hopkins was asked whether he would “agree . . . there was voluminous information that was seized in according with those search warrants for Mr. Thaler’s and Mr. Lustyik’s e-mail accounts that were nonresponsive to the search warrants?” Exhibit I at 407. He responded “Yeah. I don’t know if I would quantify it, but there was definitely information that was not responsive.” Id. He confirmed as “correct” the fact that he “never got rid of that information, [he] seized it and held on to it, but just codified it as being not relevant?” Id. Accordingly, an evidentiary hearing is needed to determine the extent of non-responsive materials seized from Mr. Thaler’s email account and iPhone and retained in this case.

the usefulness of non-responsive materials became realized as these different investigations occurred and produced new information. Id. at 360-64. Though the defense is aware of this conduct, it remains unaware of precisely which emails, texts or other items seized from the Yahoo email account or iPhone were non-responsive to the applicable search warrants. The fact that the Utah investigation focused on obstruction-related conduct, however, gives rise to a reasonable inference that evidence of a different crime, would not have been responsive.

This issue is further complicated by the June Yahoo Warrant's incorporating only Section II of Attachment B. See infra Section 3.B. In truth, no particularity is provided in the June Yahoo Warrant at all. Accordingly, how could searching agents make any informed decisions about what items to seize?

Even assuming that the list at Section III of Attachment B for the June Yahoo Warrant is sufficiently particular, or those lists incorporated and attached to the Sept. Yahoo Warrant and Sept. Residence/iPhone Warrant, they did not prevent wholesale seizure and uploading of all of Mr. Thaler's Yahoo emails and iPhone content, including those "not responsive" to the search warrants.

This Court is squarely confronted with the issue of whether the government's cavalier treatment of Mr. Thaler's Yahoo email account and the contents of his iPhone require suppression. Under these circumstances, the government is not in compliance with the search warrants for these items and has violated Mr. Thaler's Fourth Amendment protections. The seized electronic materials should, therefore, be suppressed *in their entirety*.

### III.

#### **THE GOOD FAITH EXCEPTION DOES NOT APPLY IN THIS CASE**

The good faith exception does not apply where: (1) the issuing judge was deliberately or

recklessly misled by information the affiant knew was false; (2) the issuing judge wholly abandoned his or her judicial role; (3) the supporting affidavit lacked any indicia of probable cause; or (4) the warrant was “so facially deficient – i.e., in failing to particularize the place to be searched or the things to be seized – that the executing officers cannot possibly presume it to be valid.” Leon, 468 U.S. at 923. In light of the defect above, as well as those identified in the motions already filed, the third and fourth prongs preclude application of the good faith exception because the government has failed to sustain its burden to demonstrate the objective reasonableness of the agents’ reliance on the search warrants at issue.<sup>4</sup>

**A. The June Yahoo Warrant Lacked Any Indicia of Probable Cause.**

Suppression is appropriate where probable cause is “based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.” Leon, 468 U.S. at 923. Admittedly, “[s]uch a concern most frequently arises when affidavits are bare bones, i.e., totally devoid of factual circumstances to support conclusory allegations.” United States v. Clark, 638 F.3d 89, 103 (2d Cir. 2011) (collecting cases). Mr. Thaler incorporates by reference the arguments bearing on the lack of probable cause in his main brief and set forth above. Those arguments will be repeated here.

---

<sup>4</sup> The government appears to fault Mr. Thaler for not addressing application of the good faith exception. See Gov’t Brief at 46. The Second Circuit, however, has stated that “[t]he burden is on the government to demonstrate the objective reasonableness of the officers’ good faith reliance.” George, 975 F.2d at 77 (citation omitted); see Ganas, 2014 WL 2722618, at \*9.

**B. Even if Probable Cause Exists, the Warrant Was “So Facially Deficient – i.e., in Failing to Particularize the Place to Be Searched or the Things to Be Seized – That the Executing Officers Cannot Possibly Presume it to Be Valid.”**

**1. The June Yahoo Warrant Incorporates Only “Section II of Attachment B,” Which Authorizes the Wholesale Search of Mr. Thaler’s Yahoo Email Account Untethered from Any Violation of Law.<sup>5</sup>**

The June Yahoo Warrant provides on its first page:

---

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

See Section II of Attachment B.

Exhibit A. Section II of Attachment B provides a laundry list of “property to be seized” with no reference to any criminal statute or violation. Id.

- II. Accounts and Files to Be Copied by Yahoo Personnel
- A. All data files associated with the e-mail address or account designated hannestee@yahoo.com, without limitation:
  - 1. The contents of all e-mail, whether draft, deleted, sent, or received;
  - 2. The contents of all text or instant messages;
  - 3. The contents of all electronic data files, whether word-processing, spreadsheet, image, video, or any other content;
  - 4. The contents of all calendar data;
  - 5. Lists of friends, "buddies," contacts, or other subscribers;
  - 6. Records pertaining to communications between Yahoo and any person regarding this account and any e-mail accounts associated with this address, including, without limitation, contacts with support services and records of actions taken.
- B. All subscriber and transactional records for the hannestee@yahoo.com e-mail account and any associated e-mail accounts and secondary contact e-mail accounts, including:
  - 1. Subscriber information for this and any associated e-mail accounts:
    - a. Name(s) and Yahoo account identifiers;

---

<sup>5</sup> Mr. Thaler asks leave of Court to assert this argument in his reply. He identified this particular defect in the factual recitation within the moving papers. Motion at 3. Mr. Thaler consents to and would not oppose the government filing a supplemental response to address this particular argument. In his initial motion papers, Mr. Thaler argued that the list of items to be seized in Section III was fatal to the June Yahoo Warrant’s propriety. He maintains those arguments in the alternative to this particular argument regarding the June Yahoo Warrant’s lack of particularity.

- b. Address( es);
  - c. Records of session times and durations;
  - d. Length of service (including start date) and types of service utilized;
  - e. Telephone instrument number of other subscriber number or identity, including any temporary assigned network address;
  - f. The means and source of payment for such service (including any credit card or bank account number); and
  - g. The Internet Protocol address used by the subscriber to register the account or otherwise initiate service.
2. User connection logs for any connections to or from this and any associated e-mail accounts, including:
- a. Connection time and date;
  - b. Disconnect time and date;
  - c. The IP address that was used when the user connected to the service;
  - d. Source and destination of any e-mail messages sent from or received by the account, and the date, time, and length of the message;
  - e. Any address to which e-mail was or is to be forwarded from the account or e-mail address; and
  - f. Any e-mail address that is a secondary e-mail contact for the account or for which the account serves as a secondary e-mail contact.

Exhibit A. at 4-6. All of the law governing the particularity analysis was clearly established at the time of the June Yahoo Warrant and subsequent search. It was clearly established that a warrant which fails to specify the crimes for which the search was being undertaken lacks particularity. See United States v. George, 975 F.2d 72, 76 (2d Cir. 1992); see also United States v. Vilar, No. S3 05 Cr. 621 (KMK), 2007 WL 1075041, at \*22 (S.D.N.Y. April 4, 2007) (collecting cases). It was clearly established that a warrant with unduly broad, ambiguous, or catch-all categories lacks particularity. See United States v. Buck, 813 F.2d 588, 591 (2d Cir. 1987); see also Vilar, 2007 WL 1075041, at \*22 (collecting cases). As the George Court explained, the very purpose of the particularity requirement is to “curtail[ ] the officers' discretion when executing the warrant . . . .”

975 F.2d at 76.

In appropriate circumstances a search warrant can reference other documents which may provide the requisite particularity as to the description of the items to be seized. Groh, 540 U.S. at 557. But a warrant's reference to other documents must employ “appropriate words of incorporation” to incorporate the documents into the warrant, and significantly, the referenced documents must “accompan[y] the warrant.” Id. at 557–58.

Here, the June Yahoo Warrant commanded officials to seize the items specified in “Section II of Attachment B.” But “Section II” authorized seizure quite literally of “all” items in Mr. Thaler’s Yahoo email account. Thus, the search warrant, on its face, did not describe with particularity the things to be seized as required by the Fourth Amendment.<sup>6</sup> Absent the requisite judicially-imposed restraint, the search warrant left officials executing the June Yahoo Warrant with the discretion to determine what items they would seize. Due to these defects, the June Yahoo Warrants suffers from the same lack of particularity that the Supreme Court deemed fatal in Groh, that the Second Circuit deemed fatal in George and Rosa, and that the district court so deemed in United States v. Cioffi, 668 F.Supp.2d 385, 396 (E.D.N.Y. 2009), which involved email evidence. As in those cases, the Court should suppress the evidence derived from the defective June Yahoo Warrant that was insufficiently particular. The search of Mr. Thaler’s Yahoo email account pursuant to a search warrant that failed to satisfy the particularity requirement of the Fourth Amendment is regarded as an unconstitutional, warrantless search in violation of the Fourth Amendment. Groh, 540 U.S. at

---

<sup>6</sup> Also missing from Section II of Attachment B is any temporal limitation on the items to be searched. See United States v. Hernandez, No. 09 Cr. 625, 2010 WL 26544, at \*11 (S.D.N.Y. Jan. 6, 2010) (noting that a “temporal limitation” is an “indic[ium] of particularity” (citing United States v. Capital Grp., Inc., 211 F.R.D. 31, 58 (D.Conn.2002))).

558 (citing United States v. Leon, 468 U.S. at 923).

The mere fact that Attachment B identified a purportedly more precise list of items to be seized by law enforcement at Section III does not rescue the June Yahoo Warrant. As Groh cautions, “a court may construe a warrant with reference to a supporting application or affidavit if the warrant uses appropriate words of incorporation, *and* if the supporting document accompanies the warrant.” 540 U.S. at 557–58 (emphasis added); see United States v. Rosa, 626 F.3d 56, 64 (2d Cir.2010) (“[W]e may no longer rely on unincorporated, unattached supporting documents to cure an otherwise defective search warrant.”); George, 975 F.2d at 76 (“Resort to an affidavit to remedy a warrant's lack of particularity is only available when it is incorporated by reference in the warrant itself and attached to it.”); cf. United States v. Waker, 534 F.3d 168, 172 (2d Cir. 2008) (reading a warrant as including facts set forth in an affidavit where the warrant stated: “*see attached* Affidavit as to of[sic] Items to be Seized, all of which are fruits, evidence and instrumentalities of violations of 18 U.S.C. § 922(g)(1) all of which are more fully described in the affidavit filed in support of this warrant which is incorporated herein by reference” (emphasis added)). Accordingly, though attached, nothing in the face of the June Yahoo Warrant incorporated the list of items at Section III of Attachment B. Nothing in the June Yahoo Warrant incorporated Attachment B in full either.

Moreover, the June Yahoo Warrant directs the server of the warrant to search and seize not the property described in Section III of Attachment B, but rather the property described in “Section II of Attachment B.” Thus, in this case the agent seeking the warrant did not alert Judge Alba to the defect in the warrant he had drafted “and we therefore cannot know whether [Judge Alba] was aware of the scope of the search he was authorizing.” Groh, 540 U.S. at 561, n. 4. Nor was it reasonable for the agent or any other executing official to rely on a warrant that was so patently defective, even

if Judge Alba had known of the error. Id. In other words where, as here, Section II of Attachment was incorporated into the search warrant signed by the magistrate court, the unincorporated Section III of Attachment B (and the conflicting reference to Section II) in the warrant application, put in grave doubt exactly what items the server was to search for and seize.

Granted, the government will no doubt argue that there is no problem here because the warrant that Judge Alba issued had attached to it “Attachment B,” which included Section III. Although this argument boasts an attractive appeal it suffers under the weight of the fact that the warrant does not command the server of it to seize those items. To the contrary the warrant specifically commands the server to search and seize the property in “Section II of Attachment B.”

## **2. The Exclusionary Rule Applies Due to the Lack of Particularity.**

Because the search warrant here fails for lack of particularity and is facially invalid, the circumstances of this case fall within the situation identified in Leon to which the exclusionary rule must be applied. The pivotal question in a particular case is whether a reasonably well trained officer would have known that the search was illegal despite the magistrate’s authorization. See Leon, 468 U.S. at 922 n.23. The discussion in George helps answer this question.

Reasonable reliance does not allow an officer to conduct a search with complete disregard of the warrant’s validity because the “standard of reasonableness ... is an objective one, ... [one that] requires officers to have a reasonable knowledge of what the law prohibits.” Id. at 919–20 n. 20, 104 S.Ct. at 3418 n. 20. Accordingly, the [Supreme] Court recognized that in some circumstances “a warrant may be so facially deficient— i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officer cannot reasonably presume it to be valid.” Id. at 923, 104 S.Ct. at 3421.

975 F.2d at 77. In that regard, it “requires officers to have a reasonable knowledge of what the law prohibits.” Leon, 468 U.S. at 919, n.19.

As discussed above, the law governing the particularity requirements was clearly established at the time of the June Yahoo Warrant and subsequent search. It was clearly established that a warrant which fails to specify the crimes for which the search was being undertaken lacks particularity. See George, 975 F.2d at 76; see also Vilar, 2007 WL 1075041, at \*22 (collecting cases). It was clearly established that a warrant with unduly broad, ambiguous, or catch-all categories lacks particularity. See Buck, 813 F.2d at 591; see also Vilar, 2007 WL 1075041, at \*22 (collecting cases). Coupled with Agent Hopkins' self-proclaimed experience as a Special Agent of the Department of Justice, Hopkins June Aff. at ¶ 1, as well as his submitting June Yahoo Warrant application based in part upon his "training and experience," Id. at ¶ 4, the essential principles of these cases could not have been missed by anyone experienced in the investigation of obstruction of justice, like Agent Hopkins. Id. at ¶ 1.

Here, there was nothing particular at all about the list of items at "Section II of Attachment B" or even Section III for that matter. The former called for "[a]ll data files associated with the e-mail address or account designated hannestee@yahoo.com, without limitation" to be "seized" by those executing the warrant. Exhibit A. No words could be more exhaustive or without limitation than those with regard to the search of Mr. Thaler's Yahoo email account. It is clearly tantamount to a "catchall" provision, but is not preceded by any limited list of items to be seized. Section II's failure to include criminal statute or specify the crimes by name for which the search was being undertaken makes the defects more egregious. A reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization.

Even the reference to 18 U.S.C. § 1503 in Section III of Attachment B cannot rescue the lack of particularity in the list of items at Section II. Section 1503 has been interpreted so broadly as to

garner a “catchall” characterization by the Supreme Court. See United States v. Aguilar, 515 U.S. 593, 598 (1995). Accordingly, whether reference to this statute could alter the calculus of whether a reasonably well trained officer would have known that the search was illegal despite the magistrate’s authorization is somewhat dubious at best. Cf. George, 975 F.2d at 76 (“Mere reference to “evidence” of a violation of a broad criminal statute or general criminal activity provides no readily ascertainable guidelines for the executing officers as to what items to seize”); see United States v. Leary, 846 F.2d 592, 606–10 (10th Cir.1988) (absent some other limiting feature, reference in warrant to statute covering broad range of activity facially deficient and Leon inapplicable).

In sum, the lack of particularity compels suppression under Leon. The egregious errors of law due to the lack of particularity in Section II’s list also compels suppression pursuant to Herring v. United States, 555 U.S. 135, 140 (2009), in part because it is an error of clearly established law. Judge Oetken in United States v. Zemlyansky, 945 F.Supp.2d 438 (S.D.N.Y. 2013), observed:

Groh’s logic was clear: while “our case law requires more than negligent behavior before depriving an official of qualified immunity,” this heightened culpability standard is satisfied where a warrant is so facially deficient that the executing officers cannot reasonably presume it to be valid. Id. [540 U.S.] at 565, 124 S.Ct. 1284. As one scholar noted in 2011, a natural reconciliation of the Court’s qualified immunity and criminal procedure doctrines suggests that violations of clearly established law (e.g., the conduct in Groh) will also meet the “threshold of gross negligence required by Herring.” Jennifer E. Laurin, Trawling for Herring: Lessons in Doctrinal Borrowing and Convergence, 111 Colum. L. Rev. 670, 732 (2011). After all, “[s]uch conduct is ‘gross negligence’ or recklessness, in that, as Groh also reasoned, it contravenes law so clearly established, and manifests a deficiency so apparent, that a reasonable official should have known that her actions created a high risk of constitutional harm.” Id.; see also United States v. Carroll, No. 12 Cr. 57, 2012 WL 5350364, at \*6 (E.D.N.C. Oct. 29, 2012) (“[I]f the officer may properly be charged with the knowledge that a valid search warrant contains an essential temporal component, an officer who fails to record the relevant time frame has committed a ‘deliberate, reckless, or grossly negligent’ act.” (citation omitted)).

945 F.Supp.2d at 468. Notably, Zemlyansky distinguishes between mistakes of fact and mistakes

of law in the context of whether to suppress subsequent to Herring and noted as much during this discussion. Id. at n.10.

The June Yahoo Warrant “is the type of facially invalid warrant that could not have been relied upon in good faith because ‘one who simply looked at the warrant, ... would ... suspect it was invalid.’” 975 F.2d at 78. As a result, the Leon good faith exception to the exclusionary rule does not apply.

#### IV.

#### **AN EVIDENTIARY HEARING IS WARRANTED TO RESOLVE SEVERAL FACTUAL DISPUTES**

An evidentiary hearing is required if Leon’s good faith exception is to be applied in this case. The circumstances surrounding the execution of the June Yahoo Warrant are not clear from the record. The affidavit by Agent Hopkins does not indicate that he was aware of the error in the June Yahoo Warrant discussed above. His affidavit also fails to explain what he or others executing the search warrant understood as to any limits on the search given the lack of meaningful guidelines at Section II of Attachment B. He explained that “non-presumptively privileged” files were reviewed and coded. It is unclear how they were coded, again, given the lack of meaningful guidelines at Section II of Attachment B. If officials adhered to Section II of Attachment B, every file from Mr. Thaler’s Yahoo email account would have been seized and “coded as relevant.” If officials did not adhere to Section II of Attachment B, Agent Hopkins’ affidavit is unclear as to what, if anything, was done to “particularize” the generalized and unrestrained list of items approved for seizure by Magistrate Alba. In this same vein, his testimony before the district court in Utah did not make clear what instructions were given to those officials tasked with reviewing Mr. Thaler’s Yahoo email

account returns in particular. See e.g., Mot. to Supp. Exhibit I at 348.

Furthermore, if the government intends to rely upon the statements discussed in Section A.1 above in support of any good faith argument, a hearing is needed. These statements are not included in either the Hopkins June Aff. in support of the June Yahoo Warrant or in his Affidavit attached as Exhibit M to the government's response.

Finally, a hearing is needed to resolve the extent of the error alleged pursuant to the Second Circuit's recent decision in Ganias.

**V.**

**CONCLUSION**

For these and all the foregoing reasons, the defendant, Mr. Thaler, respectfully requests that this Court grant his motions and grant any and all other relief deemed proper and fair.

Respectfully submitted,

DATED: June 20, 2014

s/ Jason I. Ser  
JASON I. SER  
Federal Defenders of New York  
Attorneys for Mr. Thaler